DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY MATERIEL COMMAND
5001 EISENHOWER AVENUE, ALEXANDRIA, VA 22333-0001

AMC SUPPLEMENT 1
to AR 380-5
CHANGE 1

6 June 1997

Security

DEPARTMENT OF THE ARMY INFORMATION SECURITY PROGRAM

This change is necessary to delegate waiver approval authority and confirm previously announced file stamping policy.

1. AMC Supplement 1 to AR 380-5, 21 April 1992, is changed as follows:

Remove old pages	**Insert new pages**
5 and 6	5 and 6

2. This change is necessary to delegate authority to approve exceptions for storage of CONFIDENTIAL and SECRET material to commanders of major subordinate commands and commanders/directors of separate reporting activities. It also confirms the elimination of the requirement to stamp file folders with the highest overall classification of material contained therein.

3. File this change in front of the supplement.

The proponent of this supplement is the United States Army Materiel Command. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to the Commander, HQ AMC, ATTN: AMXMI-SCM, 5001 Eisenhower Avenue, Alexandria, VA 22333-0001.

FOR THE COMMANDER:

OFFICIAL:

BILLY K. SOLOMON
Major General, USA
Chief of Staff

LEROY TILLERY
Chief, Printing and Publications
Branch

DISTRIBUTION:
Initial Distr H (43) 1 ea HQ Acty/Staff Ofc
LEAD (SIOLE-DO-I) (2)
AMCIO-I-SP stockroom (15)
HQDA (DAMI-POC)
AMXMI-SCM (25)

SPECIAL:
HQ IOC/AMSIO-IML (4)
ARL/AMSRL-CI-TG (4)
ATCOM/AMSAT-B-D-CARP (4)
CECOM/AMSEL-IM-BM-I (4)
CBDCOM/AMSCB-CIR (4)
LOGSA/AMXLS-IM (4)
MICOM/AMSMI-SMO (Library)(4)
SSCOM/AMSSC-S-IMS (4)
STRICOM/AMSTI-CS (4)
TACOM/AMSTA-DRM (4)
TECOM/AMSTE-CT-N (4)
USASAC/AMSAC-IM-O (4)

3. Holders of RD/FRD documents who are the proponent of the document will follow steps 1(a), 2(b), 2(c), and 2(d).

Page 21, paragraph 4-302, Photographs, films, and recordings. Add the following at the end:

If space limitations preclude use of a "DERIVED FROM" line, separate records will be maintained to identify the classifier.

Page 22, paragraph 4-305, Documents produced by ADP equipment. Add the following at the end:

A review of classification markings applied by ADP equipment will be accomplished prior to dissemination or reproduction of documents.

Page 23, paragraph 4-400, Declassification and regrading marking procedures. Add the following at the end:

Material which is automatically downgraded/declassified according to instructions on the material will be remarked, as a minimum, on the front/first page and back cover.

Page 25, paragraph 5-102a2, Storage of classified information. Add the following at the end:

Requests for approval to use alarmed areas for storage of TOP SECRET material will be forwarded through command security channels to HQ AMC, ATTN: AMXMI-SCM. Enclosures for this request will be in the format shown in appendix S to this supplement.

Page 25, paragraph 5-102b, Storage of classified information. Add the following at the end:

When classified material is proposed for open storage in vaults, buildings, offices, or rooms, qualified facility engineer personnel will verify the structural composition of the storage facility according to standards outlined in appendix H of the basic regulation. The facility will be certified regarding its composition and the highest level of classified material authorized for storage. The certification will be on a 5-year renewal basis or when there has been a physical modification to the structure.

C1, AMC Suppl 1 to AR 380-5

Page 25, paragraph 5-102b, Storage of classified information. Add subparagraphs 1, 2, 3, 4, 5, and 6.

1. CONFIDENTIAL and/or SECRET material will not be stored in steel filing cabinets equipped with a steel lock bar and secured with a GSA-approved changeable padlock.

2. Authority to approve exceptions for CONFIDENTIAL and SECRET is delegated to commanders of major subordinate commands (MSCs) of the Army Materiel Command and to commanders/directors of separate reporting activities of the Army Materiel Command. This authority may be redelegated to MSC chiefs of staff with power of redelegation to senior intelligence officers provided they are Lieutenant Colonels or GS 15s and above. Requests for waivers to TOP SECRET storage requirements will continue to be forwarded to this HQ, ATTN: AMXMI-SCM.

3. Before approving exceptions to storage standards, the approving authority should compare the construction standards of the proposed facility with those in appendix H, of the basic regulation. The construction information, combined with other factors, such as threat, sensitivity of the classified information, amount of in-depth security safeguards, and other pertinent information should be considered. Copies of approved waivers will be forwarded to this HQ, ATTN: AMXMI-SCM, with a copy furnished to AMXMI-SSD.

4. Exceptions and waivers require compensatory measures equal to or greater than the requirements of the regulation.

5. Waivers are valid for 1 year only and require annual renewal, if necessary. Approvals will be based upon submission of projects and milestones which support the attainment of the requirements of the regulations for which the waiver was issued.

6. Exceptions are permanent and are applicable only when current procedures exceed requirements of the regulation or it is cost-prohibitive to meet the requirements.

Page 26, paragraph 5-103b, Procurement and phase-in of new storage equipment. Add the following at the end:

Copies of the request will be sent to HQ AMC, ATTN: AMXMI-SCM with a copy furnished to AMXMI-SSD.

DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY MATERIEL COMMAND
5001 EISENHOWER AVENUE, ALEXANDRIA, VA 22333-0001

AMC Supplement 1
to AR 380-5

21 April 1992

Security

DEPARTMENT OF THE ARMY INFORMATION SECURITY PROGRAM

This supplement may be further supplemented by U.S. Army Materiel Command (AMC) major subordinate commands (MSC); by installations and activities reporting directly to Headquarters (HQ), AMC. Further supplementation by other organizations requires approval of Commander, HQ AMC, (AMCMI-CS). Copies of each supplement will be furnished to the Commander, HQ AMC (AMCMI-CS), and to the AMC Security Support Activity (AMXPX-S), Fort Gillem, Forest Park, GA 30050-5000.

AR 380-5, 25 February 1988, is supplemented as follows.

Page 6, paragraph 1-200, Purpose. Add the following at the end:

This supplement establishes responsibilities and procedures for administration of the AMC Information Security Program. It must be used in conjunction with the basic regulation.

Page 6, paragraph 1-201, Applicability. Add the following at the end:

This supplement applies to HQ AMC; AMC MSCs (including their subordinate installations and activities); separate installations and activities reporting directly to HQ AMC; and program/project/ product managers obtaining functional support from AMC elements.

Page 7, paragraph 1-313, Custodian. Add the following at the end:

Within AMC, the following definition applies:

Prime Custodian. The onsite chief of a division or comparable organizational element within which classified materials are maintained, the prime custodian has overall responsibility for implementing security procedures within his/her area of jurisdiction, and ensuring compliance therein.

---

*This supplement supersedes AMC Suppl 1 to AR 380-5, 12 September 1990, AR 380-5, 25 February 1988.

Page 9, paragraph 1-600c(c), Original classification authority. Add the following at the end:

Requests will be submitted through command channels to HQ AMC (AMCMI-CS). Each request will explain how conditions in paragraph 1-600c1 apply and will also provide an estimate as to the frequency with which original classification authority will be used.

Page 10, paragraph 1-602a4, Record and report requirements. Add the following at the end:

All changes will be reported promptly to HQ AMC (AMCMI-CS).

Page 10, paragraph 1-602b, Record and report requirements. Add the following at the end:

Commanders are responsible for maintaining a current list, by title, of original classification authorities in their respective organizations. AMCMI-CS will maintain a master list for the command.

Page 10, paragraph 1-603c2, Declassification and downgrading authority. Add the following at the end:

Each original classification authority will designate individuals, by position title, who are authorized to specify that information under their proponency may be downgraded and/or declassified earlier than previously specified or will specify in writing that authority is not to be further delegated. One copy of each designation and subsequent changes will be forwarded to HQ AMC (AMCMI-CS) and AMC SSA (AMXPX-S).

Page 11, paragraph 2-102, Classification planning. Add subparagraph c after subparagraph b.

c. All requests for policy and guidance will be referred through command security channels to HQ AMC (AMCMI-CS).

Page 12, paragraph 2-204g, Limitations on classification. Add the following at the end:

Requests will be submitted through command security channels to HQ AMC (AMCMI-CS).

Page 12, paragraph 2-206, Classifying documents. Add the following at the end:

If circumstances require the use of a classified subject or title, an unclassified short title will be provided for reference purposes.

Page 13, paragraph 2-302, Subsequent extension of duration of classification. Add the following at the end:

Reports will be made through command channels to HQ AMC (AMCMI-CS).

Page 14, paragraph 2-404, Review of classification guides. Add subparagraph c after subparagraph b.

c. Foreign military sales issues will be considered during the review of all classification guides.

Page 14, paragraph 2-405a, Distribution of classification guides. Add the following at the end:

Copies of each approved security classification guide (less SCI), and changes thereto, will also be sent to the addressees listed at attachment 3 to appendix E.

Page 14, paragraph 2-405b, Distribution of classification guides: Add the following:

Two copies of the approved security classification guides as specified in the basic regulation will be sent to Defense Technical Information Center (DTIC-FDAC), Cameron Station, Alexandria, VA 22304-6145.

Page 14, paragraph 2-406, Index of security classification guides. Add subparagraph c after subparagraph b.

c. One copy of each completed current DD Form 2024 (DOD Security Classification Guide Data Elements) as required by subparagraphs a and b above, will also be provided to HQ AMC (AMCMI-CS). Copies of DD Form 2024 will also be sent to Defense Technical Information Center with the guide.

Page 15, paragraph 2-701, Patent Secrecy Act. Add subparagraph d after subparagraph c.

d. A patent application that is being reviewed to determine whether or not its disclosure would be detrimental to national security will be handled according to paragraph 2-600 of this regulation. As a minimum, applications will be safeguarded in the manner prescribed for CONFIDENTIAL information.

Page 16, paragraph 3-103, Declassification by the Director of the ISOO. Add the following at the end:

Appeals will be forwarded through command channels to HQ AMC (AMCMI-CS).

Page 16, paragraph 3-202c, Systematic review procedures. Add subparagraphs 1, 2, and 3.

1. Holders of RD/FRD documents who are not the proponents of the document will--

(a) Review material to determine if it must be retained or may be destroyed.

(b) If information must be retained, develop a position regarding its classification (i.e., remain at current level, downgrade, remove RD/FRD markings, or declassify).

(c) Forward the document in question (according to procedures governing its current classification) and supporting rationale to the proponent.

2. Proponents who receive RD/FRD documents from other holders will--

(a) Review referred documents, evaluate the local position pertaining to classification, and formulate their position regarding proper classification.

(b) Mark documents to clearly indicate which portions are believed to be classified (and to what level) and which portions are unclassified.

(c) Forward documents in question (according to procedures governing its current classification) and the rationale supporting their classification position to--

Office of Classification
Mail Stop C356
U.S. Department of Energy
Washington, DC 20545

(d) Advise all holders of the results of the review by the Department of Energy.

3. Holders of RD/FRD documents who are the proponent of the document will follow steps 1(a), 2(b), 2(c), and 2(d).

Page 20, paragraph 4-205, File, folder, or group of documents. Add the following at the end:

File folders containing classified information will be stamped with the highest overall classification of material contained therein, at the top and bottom, front and back.

Page 21, paragraph 4-302, Photographs, films, and recordings. Add the following at the end:

If space limitations preclude use of a "CLASSIFIED BY" line, separate records will be maintained to identify the classifier.

Page 22, paragraph 4-305, Documents produced by ADP equipment. Add the following at the end:

A review of classification markings applied by ADP equipment will be accomplished prior to dissemination or reproduction of documents.

Page 23, paragraph 4-400, Declassification and regrading marking procedures. Add the following at the end:

Material which is automatically downgraded/declassified according to instructions on the material will be remarked, as a minimum, on the front/first page and back cover.

Page 25, paragraph 5-102a2, Storage of classified information. Add the following at the end:

Requests for approval to use alarmed areas for storage of TOP SECRET material will be forwarded through command security channels to HQ AMC (AMCMI-CS). Enclosures for this request will be in the format shown in appendix S to this supplement.

Page 25, paragraph 5-102b, Storage of classified information. Add subparagraphs 1, 2, and 3.

1. CONFIDENTIAL material will not be stored in existing steel filing cabinets equipped with a steel lock bar and secured with a GSA-approved changeable combination padlock except upon written approval of the local commander. SECRET material will also not be stored in this manner except upon written approval of the Deputy Chief of Staff for Intelligence, HQ AMC. In both instances, approval will be based upon assertion by requestor that attempts to obtain standard storage equipment have failed and that substandard storage arrangements will be upgraded as soon as possible. Written approvals will be stored in the applicable filing cabinet or security office.

2. Requests for other exceptions to storage requirements for SECRET material will be processed as prescribed in paragraph 5-102a.

3. Commanders have final approval authority for storage of CONFIDENTIAL material. They may contact Director, Intelligence Materiel Activity (AMXMI-P), Fort Meade, MD 20755-5315 for advice and assistance.

Page 25, paragraph 5-102b, Storage of classified information. Add the following at the end:

When classified material is proposed for open storage in vaults, buildings, offices, or rooms, qualified facility engineer personnel will verify the structural composition of the storage facility according to standards outlined in appendix H of the basic regulation. The facility will be certified regarding its composition and the highest level of classified material authorized for storage. This certification will be displayed inside the storage facility. The certification will be on a 5-year renewal basis or when there has been a physical modification to the structure.

Page 25, paragraph 5-102b, Storage of classified information. Add subparagraphs 1, 2, and 3.

1. Exceptions and waivers require compensatory measures equal to or greater than requirements of the regulation.

2. Waivers are valid for 1 year only and require annual renewal, if necessary. Approvals will be based on submission of projects and milestones

which support the attainment of the requirements of the regulations for which the waiver was issued. Requests for renewal will be submitted 90 days prior to the expiration date to the approval authority (HQ AMC for TOP SECRET and SECRET, local commander for CONFIDENTIAL) and will provide project/milestone status updates.

3. Exceptions are permanent and are applicable only when current procedures exceed requirements of the regulation or it is cost-prohibitive to meet the requirements. Exceptions will be reevaluated every 2 years and revalidated, as necessary. Requests for biennial review will be submitted 90 days prior to the expiration date to the approval authority (HQ AMC for TOP SECRET and SECRET, local commander for CONFIDENTIAL).

Page 26, Paragraph 5-103b, Procurement and phase-in of new storage equipment. Add the following at the end:

Copies of the request will be sent to HQ AMC (AMCMI-CS) with a copy furnished to AMC SSA (AMXPX-S).

Page 26, paragraph 5-104b3(a), Designations and combinations. Add the following at the end:

Only one Standard Form 700 (Security Container Information) will normally be affixed to the inside of each security container. If a security container has drawers which are equipped with a separate external locking device and the custodians are not the same for all drawers, a separate SF 700 will be displayed in each drawer. If each drawer has the same prime custodian, then a copy of part 2 of the original SF 700 or a duplicate will be placed inside each drawer.

Part 1, SF 700 will be used to list the names of the personnel to be contacted in an emergency. These individuals need not know the combination, nor must all the individuals who know the combination be listed on part 1.

Page 26, paragraph 5-104b3(b), Designations and combinations. Add the following at the end:

Part 2, SF 700 will be used to list all those people having knowledge of the combination. The names listed on parts 1 and 2 of the SF 700 need not be the same.

Page 28, paragraph 5-202a2, End-of-day security checks. Add the following at the end:

When checking a safe with conventional type combination dial, check each drawer individually by depressing drawer latch and pulling. Rotate combination dial at least four times in one direction and re-check each drawer. When checking a safe with manipulation proof dial combination, reset

the dial to 0 and turn the butterfly to the right to relock it and move the dial to the right until it stops. Then press down on latch of combination drawer and pull out on it at the same time. Keep the latch down on the combination drawer while checking the other drawers. After completing the check, unlock the butterfly and rotate the dial at least four times in one direction.

Page 28, paragraph 5-202e2, End-of-day security checks. Add subparagraphs 3 and 4.

3. After duty hours inspections will be routinely conducted to ensure compliance with all applicable regulations. The security manager will ensure that local rules for conducting after duty hour inspections are established.

4. Room check procedures will be established in each separate office where classified information/materiels are used or stored. SF 701 (Activity Security Checklist) will be posted near the office exit door and will be used to certify completion of the room check each duty day.

Page 28, paragraph 5-203a, Emergency Planning. Add the following at the end:

Emergency plans will be reviewed every 2 years.

Page 29, paragraph 5-203h, Emergency planning. Add the following at the end:

All requests will be sent to HQ AMC (AMCMI-CS).

Page 29, paragraph 5-205a, Security of meetings and conferences. Add the following at the end.

This headquarters has the authority to approve classified conferences that are held in a cleared facility, involve U.S. personnel exclusively, and are not acquisition related. Classified conferences involving foreign participation, or that are acquisition related, or are scheduled to be held in an uncleared facility must be forwarded through this headquarters, ATTN: AMCMI-CS to HQDA, DAMI-CIS, for approval. Classified conferences that are sponsored or co-sponsored by a nongovernmental association must be forwarded through AMCMI-CS and HQDA to Department of Defense (DOD) for approval; the application must contain a security plan.

Page 31, paragraph 5-205f3, Security of meetings and conferences. Add the following at the end:

All requests submitted under the provisions of this chapter will be routed through command security channels to arrive at HQ AMC (AMCMI-CS) 150 days prior to the conference. Emergency requests will be accepted when justified.

Page 31, paragraph 5-205g2, Security of meetings and conferences. Add the following at the end:

Proposals to exclude foreign nationals, when appropriate, will be forwarded through command security channels to HQ AMC (AMCMI-CS) for approval by HQDA (DAMI-CIT).

Page 31, paragraph 5-206f, Safeguarding of U.S. classified information located in foreign countries. Add the following at the end:

Requests will be sent through command security channels to HQ AMC with a copy furnished to AMC SSA (AMXPX).

Page 31, paragraph 5-300, Policy. Add the following to subparagraph a:

MSCs and separate reporting activities who have classified material will establish an entry and exit program designed to deter or detect unauthorized introduction or removal of that material. Tenant activities are not required to establish a separate inspection program, provided this service is conducted by the host organization. This requirement should be incorporated in the DD Form 1144 (Support Agreement). In addition, tenant activities must ensure the scope and conduct of inspections conform to the requirements of this supplement and AR 380-5.

Page 32, paragraph 5-300, Policy. Add the following to subparagraph g:

A detailed standing operating procedure (SOP) will be developed at each installation/activity for the conduct of the inspections. If required, the SOP will be coordinated with local unions, legal and law enforcement personnel. Signs will be posted notifying employees and visitors that they are subject to a handcarried container search.

Page 32, paragraph 5-300, Policy. Add subparagraph i after subparagraph h.

i. Where possible, the inspection program will be carried out in the areas where classified work is performed.

Page 32, paragraph 5-300, Policy. Add subparagraphs j, k and 1:

(j) Actions to be taken in the event contraband or controlled substances are found. In the event that contraband or controlled substances are found during the inspection, the individual(s) will be detained and appropriate law enforcement officials will be notified. Such officials will be identified in the SOP. Inspection personnel will keep the contraband or controlled substance in their possession until turned over to law enforcement personnel in order to comply with the chain-of-custody rule for evidence.

(k) Personnel who may be used to perform entry/exit inspections. Personnel that may be used to perform this function include military police, DOD guards, contract guards, DOD security personnel or Department of the Army (DA) civilian personnel appointed by the commander or director. Prior to performing the inspection, all personnel will be thoroughly trained.

(l) Steps to be taken in the event of refusal to submit to inspection. In a restricted area, in the event anyone refuses to submit to the inspection, the individual must be properly identified. This can be done by taking the information from their badge or requesting them to produce an identification (ID) with a picture on it (such as a state driver's license). Consistent with security needs take reasonable actions to obtain identification. If an identified individual still refuses to submit to the inspection, he/she will be informed that a report of the incident will be made and he/she could be subject to a disciplinary action and barred from entering the installation/ building in the future. Force will not be used to enforce the inspection on any individual without probable cause that would lead the inspector to believe that the individual has unauthorized classified material in his/her possession.

Page 32, paragraph 5-301, Inspection frequency. Add the following to subparagraph a:

Commanders of MSCs and separate reporting activities (SRA) will take into consideration the threat, vulnerabilities, sensitivity of classified information, and locations in determining the frequency of inspections.

Page 32, paragraph 5-301, Inspection frequency. Add subparagraph g after subparagraph f:

g. Inspections are to be conducted in locations where classified material is stored or worked on (rather than at other locations such as vehicle gates). The inspections will be frequent enough to provide a credible deterrent against theft of classified material. As a minimum, inspections will be conducted at least 2 hours per quarter.

Page 33, Paragraph 5-303, Local records. Add subparagraph d after subparagraph c.

d. The information required by this paragraph (dates and numbers of inspections, number of instances in which persons handcarried classified information without apparent authorization, and problems encountered in the entry/exit inspection program) will be attached as an addendum to the Annual Information Security Program Data Report (SF 311). MSCs will consolidate the information prior to forwarding it to this headquarters.

Page 33, paragraph 6-102, Responsibility of discoverer. Add subparagraph d after subparagraph c.

d. Some examples of instances that must be reported to the security manager include discovery of any of the following:

1. TOP SECRET documents lost to accountability.

2. Security container open and unattended.

3. Classified documents left unsecured and unattended.

4. Disclosure of classified information to a person not authorized access.

5. Appearance of classified material in public media.

6. Classified information discussed or sent over an unsecure means of communication.

Page 33, paragraph 6-103, Preliminary inquiry. Add the following:

The inquiry, including the written report, will be completed as quickly as possible but in no case will it exceed 30 days after discovery of the security incident. Progress of the preliminary inquiry will be monitored by the local security manager who will provide the commander with the written results. Each MSC/SRA will establish a uniform system for numbering preliminary inquiries (i.e., AMC 1-92). These numbers will be on a fiscal year basis. These numbers will be used to identify violations reported as part of each subsequent Security Status Report and will use the recommended format provided at appendix Q to provide updates until the case is closed through assignment of either administrative or disciplinary action or a determination that no such action is warranted. This will be accomplished even when investigation eliminates the possibility of compromise or establishes that compromise could not reasonably be expected to cause damage to national security. Preliminary inquiries may be conducted by security specialists, regardless of grade, provided the inquiries are conclusive and the findings and recommendations are approved at the chief of staff or equivalent level.

Page 33, paragraph 6-103c1, Preliminary inquiry. Add the following:

Copies of the report will be provided through command security channels to HQ AMC (AMCMI-CS).

Page 34, paragraph 6-104g, Investigation. Add the following at the end:

Investigating officers will not specify the nature of any disciplinary action to be taken. This will be determined by the responsible individual's immediate supervisor and the civilian/military personnel officer according to applicable regulations.

Page 34, paragraph 6-104h, Investigation. Add the following at the end:

Security managers will establish procedures for the timely and efficient conduct of investigations within their organizations. Security managers of MSCs will monitor the progress of investigations conducted by subordinate elements.

Page 34, paragraph 6-105a, Responsibility of authority ordering investigation. Add the following at the end:

This review will be conducted by the security manager and staff judge advocate or other legal counsel.

Page 34, paragraph 6-105d, Responsibility of authority ordering investigation. Add the following at the end:

In such cases one copy of the report of investigation will be forwarded to HQ AMC (AMCMI-CS).

Page 34, paragraph 6-105f, Responsibility of authority ordering investigation. Change to read:

Each MSC and SRA will forward one copy of approved reports of investigation involving TOP SECRET and SECRET information to HQ AMC (AMCMI-CS).

Page 35, paragraph 6-111, Suicide and attempted suicide. Add the following at the end:

Within 3 workdays following a suicide, the cognizant security manager will forward preliminary results of the inquiry to Commanders, HQ AMC (AMCMI-CS). The report will include--

a. Individual's name and grade/rank.

b. Level of security clearance.

c. Frequency of access to classified information.

d. Frequency with which the individual worked alone with classified materials (including overtime).

e. Whether or not there appears to be any missing classified documents or whether or not classified material expected to be in the individual's possession can be accounted for.

f. All other pertinent facts.

g. This information may be included in the serious incident report (SIR), provided HQ AMC, ATTN: AMCMI-CS is included as an addressee.

Page 35, paragraph 6-112c, Unauthorized disclosure of classified information to the public. Add the following at the end:

"Information copies" of the report will be sent to CDRAMC ALEX VA //AMCMI_CS//.

Page 36, paragraph 7-lOObl, Policy. Add the following at the end:

Within AMC, the brief period of time during which one individual with access may be left alone should not exceed 15 minutes. Organizations storing TOP SECRET or Special Access Program (SAP) information must establish physical controls that will preclude one person from having access to the information during nonduty hours. Establishing a written policy that prohibits one individual from accessing the information during nonduty hours does not satisfy this requirement.

Page 36, paragraph 7-101, Access by persons outside the Executive Branch. Add the following at the end:

This paragraph pertains only to individuals and agencies within the U.S. Government, but outside the Executive Branch. For personnel within the Executive Branch, no special authorization is required. Access by those individuals and agencies outside the Executive Branch is governed by the basic regulation.

Page 36, paragraph 7-101d2, Access by persons outside the Executive Branch. Add the following at the end:

Requests will be forwarded through HQ AMC (AMCMI-CS).

Page 37, paragraph 7-105b, Access by visitors. Add the following at the end:

AMC Form 1663-R-E (Request for Visit Authorization) will be used for visit requests. A copy of the form is attached at appendix T.

Page 38, paragraph 7-106b, Student officers attending civilian institutions and faculty members of civilian institutions. Add the following at the end:

Requests will be forwarded 120 days before intended access and if possible through HQ AMC (AMCMI-CS). They will include--

a. Individual's name, date/place of birth, social security number, and citizenship.

b. How the individual is affiliated with DOD.

c. Name of individual's employer and employment location.

d. Level of access required and inclusive dates.

e. Current security clearance, if any; past security clearance(s); and any other indications that the individual is trustworthy.

f. Inclusive dates and branch of prior military service, if known.

g. Full justification for disclosing classified information to the individual.

h. Subject matter of disclosure.

i. Explanation as to why access is in the best interest of national security.

j. Explanation as to how the individual will safeguard classified information from unauthorized disclosure.

k. Point of contact with phone number and security manager's phone number.

Page 39, paragraph 7-300a, TOP SECRET information. Add the following:

Requests for waivers of the minimum rank/grade for TOP SECRET control officers will be forwarded to this headquarters, ATTN: AMCMI-CS for approval.

Page 39, paragraph 7-300b1(d), TOP SECRET information. Add the following at the end of the paragraph:

TOP SECRET pages that are superseded by changes will be recorded on a destruction certificate and the annotation of the destruction certificate will be witnessed.

Page 39, paragraph 7-300b1(e), TOP SECRET information. Add the following at the end:

TOP SECRET document accounts will be recorded on DA Form 455 (Mail and Document Register) or DA Form 3964 (Classified Document Accountability Record). The register for any given calendar year will be retired after the appropriate dispatch or destruction of all TOP SECRET documents listed. The retired register(s) will be maintained in the current files for 5 years and then destroyed.

Page 39, paragraph 7-300c1, TOP SECRET information. Add the following at the end:

The report of inventory will contain a listing of local control numbers. The signed certification of inventory will attest that inventoried documents were physically sighted and were complete.

Page 39, paragraph 7-300c2, TOP SECRET information. Add the following at the end:

AMC installations and activities with more than 100 TOP SECRET documents will conduct a 10 percent physical inventory each month until all TOP SECRET documents have been accounted for. Those with 100 or less are exempt from the 10 percent inventory. Inventories will be completed by April of each year.

Page 39, paragraph 7-300e, TOP SECRET information. Add the following at the end:

DA Form 3964 will be used for this purpose. The description of the document must be consistent with that which appears on the applicable DA Form 969 (TOP SECRET Document Record) or another approved document register.

Page 40, paragraph 7-301, SECRET information. Add the following at the end:

Within AMC, administrative control procedures other than those required by the basic regulation or other DA regulation or directives are prohibited.

Page 40, paragraph 7-303, Receipt of classified material. Add the following at the end:

Only mail bearing the caveat "POSTMASTER: Address Correction Requested/Do Not Forward" needs to be afforded this protection.

Page 40, paragraph 7-304c, Working papers. Add the following at the end:

Requests for waivers will be submitted through command channels to HQ AMC (AMCMI-CS).

Page 41, paragraph 8-101, TOP SECRET information. Add the following at the end:

TOP SECRET information destined for DOD contractors will not be dispatched until storage capability and facility clearance have been verified.

Page 41, paragraph 8-i02, SECRET information. Add the following:

SECRET information destined for DOD contractors will not be dispatched until the safeguarding capability, facility clearance, and classified mailing address have been verified. SECRET information may be transmitted via United States Postal Service Express Mail within the 50 states, District of Columbia, and Puerto Rico.

Page 41, paragraph 8-103, CONFIDENTIAL information. Add the following:

CONFIDENTIAL information destined for DOD contractors will not be dispatched until facility clearance, safeguarding capability, and classified mailing address have been verified.

Page 44, paragraph 8-201, Addressing. Add the following:

When transmitting classified items to contractors, a person's name may not be used in the attention line of the outside envelope.

Page 44, paragraph 8-202d5(a), Receipt systems. Add the following at the end:

DA form 3964 may also be used to acknowledge receipt of classified hardware.

Page 44, paragraph 8-203, Exceptions. Add the following at the end:

Requests will be forwarded through HQ AMC (AMCMI-CS).

Page 46, paragraph 8-303b, Authority to approve escort or handcarry of classified information aboard commercial passenger aircraft. Add the following:

DA officials who have been authorized to approve travel orders may designate couriers to handcarry classified information to outside continental United States (OCONUS) locations aboard U.S. military conveyances, provided such transportation is used exclusively, and all other applicable portions of this chapter are adhered to. This authority also permits the courier to handcarry

the items within the OCONUS area. The commander, HQ AMC, and his single designee, the Deputy Chief of Staff for Intelligence, have been authorized to approve the handcarry of classified information on commercial aircraft outside the area encompassed by the boundaries of the United States, its territories, and Canada. The use of foreign flag carriers must be specifically justified. Requests will be submitted by an electrical message or DATAFAX through command security channels to Commander, HQ AMC (AMCMI-CS), at least 5 workdays before travel. As a minimum, such messages will be protected as FOR OFFICIAL USE ONLY until completion of classified courier duties. Requests will contain all information required by subparagraphs 1 through 4, basic regulation, and will additionally explain why materials cannot be transmitted by secure message or facsimile. Requests for return trip handcarry need to be justified. NOTE: HQ AMC authorization is not required to handcarry classified information to Canada or U.S. Territories. Local travel approving officials may authorize handcarry in those instances.

Page 46, paragraph 9-100, Policy. Add the following at the end:

Each commander is responsible for ensuring that destruction officers and disinterested witnessing officials for TOP SECRET materials are appointed. A sufficient number of individuals will be so designated to ensure the availability of officials for timely destruction. Security clearances must be verified before destruction and witnessing officials are designated to perform those functions.

Page 47, paragraph 9-103b, Records of destruction. Add the following at the end:

DOD policy requires that classified information intended for destruction is actually destroyed. Within AMC, two procedures are authorized for destruction of SECRET information-- Execution of a destruction certificate, one signature ONLY required. Imposition of the two-person rule, destruction certificate not required. To comply with the two-person rule, local procedures should be developed to ensure that two cleared persons are involved in the entire destruction process. Within AMC, compliance with this requirement is assumed provided the destruction process is conducted in an area occupied by the individual accomplishing destruction and at least one other cleared individual. Records of destruction are permitted only for those documents/material for which formal accountability procedures have been prescribed. Destruction of classified material will be administered in the same manner as for documents, including completion of DA Form 3964, when required.

Page 47, paragraph 9-105b, Classified document retention. Add the following at the end:

The annual cleanout date for AMC installations and activities will be during the fourth quarter of each calendar year. Local commanders will determine the exact date based upon mission requirements. The date chosen will be indicated in item 12, Remarks, SF 311, Agency Information Security Program Data Report.

Page 47, paragraph 10-101g, Scope and principles. Add the following at the end:

This includes "talking around" classified information and devising personal codes/codewords in order to obscure the true meaning.

Page 47, paragraph 10-101, Scope and principles. Add subparagraph n after subparagraph m:

n. The Security Education Program will consist of the following elements:

1. An Indoctrination briefing which is an individual briefing by a supervisor or security representative and is given before granting access to classified information to ensure that newly assigned employees know the job-specific security requirements and security procedures for the office. More emphasis on security procedures will be needed when the new employee has not had previous experience handling classified information (e.g., explanation of levels of classified material, basic marking requirements, need-to-know, storage, and reporting breaches of security should be presented). This briefing may be supplemented, but not replaced, by a requirement to read applicable security regulations.

2. An orientation briefing which is a group briefing, scheduled on a regular basis, for new personnel who have access to classified information. The briefing will cover items in subparagraphs 10-101a through 10-101m. The activity turnover rate will dictate the size of the audience and frequency of the briefing.

3. Refresher training requirements are outlined in paragraph 10-101 of the basic regulation. Not all of the items listed in this paragraph must be formally briefed to all personnel annually. Items from this list will be selected to fit the needs of the audience and local requirements.

4. Foreign travel. (See paragraph 10-104, basic regulation.)

5. Termination briefings. (See paragraph 10-105 basic regulation and AMC Suppl 1.)

Page 48, paragraph 10-103, Refresher briefings. Add the following at the end:

Refresher briefings will be conducted at least annually. Such training may combine security awareness training, Operations Security (OPSEC) training (required by AR 530-1), and Subversion and Espionage Directed Against U.S. Army (SAEDA) training. Requiring that individuals read security regulations and then certify their understanding of the requirements does not satisfy training requirements. Appendix R contains a list of suggested topics for briefings; security manager involvement in identifying other topics for specific audiences is recommended.

Page 48, paragraph 10-105a, Termination briefings. Add the following:

Security Termination Statements will be executed only when required by the basic regulation. For example, a Security Termination Statement need not be executed for an employee transferring from one DOD office to another when it is known that the employee's new position will require a security clearance.

Page 49, paragraph 10-106, Other requirements. Add subparagraph c after subparagraph b:

c. Records will be maintained on file to document attendance for all briefings outlined in paragraph 10-101n of this supplement. For annual refresher briefings, records will, as a minimum, consist of name, organizational element, date of training/briefing, and type of briefing. The refresher briefing records will be maintained until completion of the next year's training program.

Page 52, paragraph 13-200c, Management responsibility. Add the following at the end:

Requests for exceptions to the basic regulation or this supplement will be forwarded through command security channels to Commander, HQ AMC (AMCMI-CS).

Page 52, paragraph 13-301, Military departments. Add the following at the end:

The HQ AMC Deputy Chief of Staff for Intelligence is responsible for implementation of and compliance with DOD and Department of the Army Information Security Program requirements throughout AMC. The Chief, AMC SSA, is responsible for monitorship (through inspections) of the AMC Information Security Program.

Page 53, paragraph 13-304a1, Field program management. Add subparagraph (i) after subparagraph (h):

(i) Initiate and supervise measures to ensure classified holdings are kept to a minimum consistent with mission accomplishment.

Page 53, paragraph 13-304c1, Field program management. Add subparagraphs (m), and (n) after subparagraph (1):

(m) Provide a quarterly security status report AMCMI-302 (appendix Q) to Commander, HQ AMC (AMCMI-CS). Reports will be provided no later than 15 January, 15 April, 15 July, and 15 October of each year and will cover the preceding quarter. AMC MSCs will provide consolidated reports.

(n) Monitor progress of preliminary inquiries and investigations into security violations.

Page 54, paragraph 14-101b2, Violations subject to sanction. Add the following at the end:

CPR 700 (C14), 751.A, appendix A, Tables Pertaining to Penalties for Various Offenses, should be consulted by individual's supervisor for general guidance.

Page 62, appendix C, paragraph 2a(3), Policy and procedure. Add the following at the end:

Requests for code words will be submitted in writing to Commander, HQ AMC, (AMCMI-S).

Page 62, appendix C, paragraph 2b(5)(c), Nicknames. Add the following at the end:

Requests for nicknames and notification of cancellation of assigned nicknames will be submitted in writing to Commander, HQ AMC (AMCMI-S). Nicknames will expire 1 year from effective date of issuance unless otherwise requested in writing by the nickname sponsor.

Page 116, appendix D, section 1, paragraph 2, Authority. Add the following at the end:

Information classified pursuant to this guide will be safeguarded according to this regulation.

Page 117, appendix D, section 1, paragraph 6, Public Release. Add the following at the end:

AMC guides will contain the following statement:

"Within the Department of the Army, procedures specified in AR 360-5 will be followed. Defense contractors will comply with DOD 5200.22M and other contractual requirements. For those agencies under cognizance of the U.S. Army Materiel Command, all information concerning (title of system, project, program or item), will be forwarded for public clearance to (name and address of clearance authority) according to AR 360-5, paragraph 9-2. Material submitted for clearance through U.S. Army Materiel Command (when required) will be forwarded to the Commander, HQ AMC (AMCPA), 5001 Eisenhower Avenue, Alexandria, VA 22333-0001, prior to public release."

Page 122, appendix D, section 8, Hardware. Add the following:

a. Notes will be used when appropriate but are not required. Guides should be written in an easy-to-read manner and will not include any data that is not applicable to the time or system for which the guide is written.

b. A mandatory review is required every 2 years for all guides; the date 2 years after the approval date will be the suspense date for this review. However, prompt action will be taken when any regrading becomes appropriate,

even during the staffing and coordination phases. Foreign military sales issues will be addressed in the review of all guides regardless of whether item is currently being considered for sale.

c. If no changes are required as a result of the review, the originator (action officer) will place a notation on the record copy of the guide attesting to the review and affixing his/her signature and date thereto.

d. Whenever minor changes are required (as the result of review or change in status of item) an addendum to the security classification guide will be prepared, using the format in attachment 1, this appendix.

e. A sample format for Materiel Status Submission is shown in attachment 2, this appendix.

f. Security managers and persons responsible for writing security classification guides should develop a standard listing of categories of information to be included in security classification guides as they pertain to missions, munitions, radars, and other major items of AMC responsibility.

g. Initial Operational Capability (IOC) dates may only be classified when--

1. Previously released unclassified items of information such as testing schedules, dates for production decisions, production or delivery schedules, or production preparation date will not compromise the IOC dates. If IOC dates must be classified, the declassification date should be a specific, finite date or Originating Agency's Determination Required (OADR).

2. Disclosure of the IOC dates would cause damage to the national security.

Page 123, appendix E, Format variations. Add attachments 1, 2, and 3 at the end:

Page 141, appendix P. Add appendixes Q, R, S and T after appendix P.

The proponent of this supplement is the United States Army Materiel Command. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to the Commander, HQ AMC, ATTN: AMCMI-CS, 5001 Eisenhower Avenue, Alexandria, VA 22333-0001.

FOR THE COMMANDER:

OFFICIAL:

WILLIAM B. McGRATH
Major General, USA
Chief of Staff

LEROY TILLERY
Chief, Printing and Publications
Branch

DISTRIBUTION:
Initial Distr H (60) 1 ea HQ Acty/Staff Ofc
B LEAD (5,875)
AMCIO-I-SP stockroom (75)
HQDA (DAMI-CIS)
AMCMI-CS (50)

Attachment 1 to Appendix E

SAMPLE FORMAT FOR ADDENDA TO SECURITY CLASSIFICATION GUIDES

LETTERHEAD OF PROPONENT

MSR No. (To be provided by AMCRD-O)

Date

ADDENDA

SUBJECT: _____ Security Classification Guide

Page	Para	Change
		Provide narrative explanation of change, i.e., item has been upgraded/downgraded to _____ or declassified, effective _____ date

(SIGNATURE BLOCK)

Attachment 2 to Appendix E

SAMPLE FORMAT FOR MSR SUBMISSION

(LETTERHEAD OF PROPONENT)

(Office symbol) (Date)

MSR: (To be completed by AMCRD-O)

SUBJECT: Materiel Status Record Submission

Commander
U.S. Army Materiel Command
ATTN: AMCRD-O
Alexandria, VA 22333-0001

The following record of approved security classification guide, together with attached document, is forwarded for recording in the Materiel Status Record according to AR 70-2.

GENERAL INFORMATION

a. Project title:

b. Project number:

SECTION 3 - SECURITY CLASSIFICATION GUIDE

a. Subject:

b. Issued by:

c. Approval date:

d. Action officer: DSN:

e. Supersessions: (Date)

FOR THE COMMANDER:

1 Encl
Guide (dupe)

(Signature Block)

Attachment 3 to Appendix E

DISTRIBUTION OF SECURITY CLASSIFICATION GUIDES

Copies of each approved Security Classification Guide (less SCI) and changes thereto will be distributed as follows:

a. Chief, AMC SSA (AMXPX-S) (1).

b. Commander, AMC (AMCMI-CS) (1).

c. Commander, USA Materiel Readiness Support Activity (AMXMD-PQ), Lexington, KY 40511 (1).

d. HQDA element having staff jurisdiction over the item (1).

e. Commander, U.S. Army Test and Evaluation Command (AMSTE-SI-S), Aberdeen Proving Ground, MD 21005 (2).

f. Director, U.S. Army Materiel Systems Analysis Activity (AMXSY-PS), Aberdeen Proving Ground, MD 21005 (1).

g. Commander, AMC (AMCRD-O) (2) by letter in format shown in attachment 2 to appendix E of this supplement.

h. If applicable, to Depot Systems Command for provision to the security manager of the depots where storage and repair of the end item is anticipated (1).

i. Commander, AMC (AMCRM-BC-S) (1).

j. Commander-in-Chief, U.S. Army Europe and Seventh Army (AEAGC-FMD), APO New York 09403 (1).

k. Commander, Military Traffic Management Command (MT-SS), Nassif Building, 5600 Columbia Pike, Falls Church, VA 22041 (1).

l. Commander, Forces Command (AFOP-FM), Fort McPherson GA 30330 (1).

m. Commander, Training and Doctrine Command (ATCD-D), Fort Monroe, VA 23651 (1).

n. Commander, U.S. Army Pacific (APIN-SC), Fort Shafter, HI 96858 (1).

o. Defense Technical Information Center, (DTIC-FDAC), Cameron Station, Alexandria, VA 22304-6145 (2).

(The following are classification examples and are not valid guidance for any effort.)

FOREIGN MILITARY SALES ISSUES	CLASS	DECLASS	REMARKS
(1) Highest level of classified information that could be disclosed by sale of end item.	S	OADR	See note*
(2) Highest level of classified information that must be disclosed to enable production of end item.	S	OADR	See note*
(3) Highest level of classified information that must be disclosed by operation of the end item.	C	OADR	
(4) Highest level of classified information that must be disclosed in the maintenance of the end item.	C	OADR	
(5) Highest level of classified information that must be disclosed in training to use the end item.	C	OADR	
(6) Highest classification of information that could be revealed by reverse engineering the end time.	S	OADR	
(7) Highest classification of information that could be revealed by testing the end item.	S	OADR	

*Above additional elements should be considered for inclusion in the revision of the next DOD 5200.1-H and listed in Section 7. Administrative Data.

APPENDIX Q

RECOMMENDED FORMAT FOR SECURITY STATUS REPORT

(Requirement Control Symbol AMCMI-CS-302)

_____Quarter FY_____

1. Security violations attributable to reporting activity. (AR 380-5, chapter VI.)

a. Number of preliminary inquiries/formal investigations initiated for violations attributable to this activity during the reporting period: _____.

b. Following narratives will be identified by the security violation number assigned pursuant to paragraph 6-103, AMC Suppl 1 to AR 380-5.

c. Provide a brief narrative for each inquiry/investigation initiated during the quarter and identified above. Indicate highest level of classification involved. If investigation is complete, address findings as to the probability of compromise and possibility of damage to National security. Specify what disciplinary action (if any) was taken against responsible individual(s). If responsible individual(s) have been cited for other security violations during the past 2 years, identify date(s) and nature of those prior violations.

d. Provide a brief narrative of results of inquiries/investigation which were completed during the quarter, but were initiated in a prior quarter (specify quarter in which violations occurred).

2. Security awareness. (Report refresher training only. Do not include initial orientations.)

a. General Security Education (AR 380-5, chapter X).

(1) Number eligible during the year _____.

(2) Number trained during the quarter _____.

(3) Number trained during the year _____.

b. Operations Security (OPSEC) Training (AR 530-1).

(1) Number eligible during the year _____.

(2) Number trained during the quarter _____.

(3) Number trained during the year _____.

c. Subversion and Espionage Directed Against U.S. Army (SAEDA) Training (AR 381-12).

(1) Number eligible during the year _____.

(2) Number trained during the quarter by--

(a) AMC _____.

(b) INSCOM _____.

(3) Number Trained during the year by--

(a) AMC _____.

(b) INSCOM _____.

(4) Number of SAEDA training sessions conducted during the quarter by--

(a) AMC _____.

(b) INSCOM _____.

(5) Number of SAEDA training sessions conducted during the year by--

(a) AMC _____.

(b) INSCOM _____.

3. TOP SECRET document holdings. Report only those documents maintained under local accountability (paragraph 13-304, basic regulation). Do not include documents maintained within special security offices or microfiche maintained under the DOD Scientific and Technical Intelligence Information Support Program.

(a) Total on hand at end of last quarter: _____.

(b) Total on hand at end of this quarter: _____.

(c) Total received or originated during this quarter: _____.

(d) Total destroyed, transferred, or downgraded during this quarter: _____.

4. Remarks. Identify all actions taken locally during this quarter to improve indicators reported above. Also, explain all figures which are inconsistent with previous report.

_____.

5. Point of contact. Provide name and telephone number of person(s) to be contacted concerning this report _____.

APPENDIX R

SUGGESTED TOPICS FOR BRIEFINGS

TRAINING TOPIC

	Mgr	Supv	Clerical	Compu-ter	Mail Distr
Technology transfer	X	X		X	X
Unauthorized disclosures	X	X		X	X
Levels of classification	X	X	X	X	X
Original classification	X				
Derivative classification	X				
Challenges to classification	X				
Effects of open publication	X				
Classification/declassification instructions	X	X	X	X	
Marking documents/other items	X	X	X	X	X
Tentative classifications	X	X	X	X	
Combinations	X	X	X	X	X
Storage/safeguarding (incl computer media)	X	X	X	X	X
Care during duty hours	X	X	X	X	X
Violations/compromise - discovery	X	X	X	X	X
Handling NATO, RD, FRD, CNWDI, TOPSECRET	X	X	X	X	X
Telephone line transmission security	X	X	X	X	X
End-of-day checks	X	X	X	X	X
Working papers	X	X	X	X	
Security classification guides - use	X	X		X	
Visits by contractors	X	X		X	
Working with accredited foreign personnel	X			X	
Handcarrying classified material	X	X	X	X	X
Foreign government information	X	X		X	X
Third agency rule	X	X		X	X
Meetings and conferences	X	X	X	X	
Clearance of speeches/papers	X	X	X	X	
Foreign disclosure program	X	X		X	
Industrial security	X	X		X	
Security classification guides - preparation		X			
Removal of classified during nonduty hours	X		X	X	X

	Mgr	Supv	Clerical	Compu-ter	Mail Distr
Need-to-know	X	X	X	X	X
FOUO	X	X	X	X	
Personnel security clearances	X	X		X	
Briefing requirements	X	X		X	
Position sensitivity	X	X	X	X	
Typing/wordprocessing precautions		X	X	X	
Inventories		X	X	X	
Destruction		X	X	X	
DD Form 254		X		X	
Warning notices			X	X	
Compilations			X	X	
Downgrading documents			X	X	
Upgrading classifications			X	X	
Reproduction			X	X	X
Transmission			X	X	X
Packaging			X	X	X
Receipts			X	X	X
Custodial duties			X	X	X
Effects of open publication				X	

SPECIALIZED GROUPS (including engineer, contracting, finance, public affairs, personnel, etc.) are sometimes overlooked in tailoring security topics to their specialized needs. Ensure that briefings for groups such as these are prepared in a similar manner to those for the larger groups addressed above.

APPENDIX S

RECOMMENDED FORMAT FOR REQUESTS FOR EXCEPTIONS TO STORAGE REQUIREMENTS

Provide answers to the following items using narrative format, including all pertinent details. Yes or no answers should be used only when data in narrative forms is not applicable. Attach blueprints, drawings, and sketches when possible. Recently conducted physical security surveys may assist in completion of items. Completed reports may be considered For Official Use Only; occasionally classification may be warranted.

SECTION A - GENERAL

1. Name of facility.

2. Facility location and room(s).

   Building number (if any).
   Geographic location.

3. Responsible officer.

   Alternate.
   Telephone (commercial and Defense Switched Network (DSN)).

4. Type of facility.

   a. Class A Vault.

   b. Class B Vault.

   c. Class C Vault.

   d. Alarmed area.

   e. Total square feet facility occupies.

   f. Kind and classification of material to be protected (documents, hardware, magnetic media, etc.).

   g. Duty hours _____ to _____, number of days per week _____.

   h. Construction/modification is complete (yes) (no), anticipated date of completion is _____.

SECTION B - PERIPHERAL SECURITY

5. Description of surrounding area outside of building.

   a. Fence.

   b. Fence lighting.

   c. Fence guards.

   c. Relationship of building to surrounding area.

6. Building.

   a. Construction.

   b. Building access control (continuous or during security hours only).

   c. Guards (military) (civilian).

      (1) Clearance.

      (2) Frequency of checks.

      (3) Communications.

      (4) Emergency procedures.

      (5) Reserves.

7. Remarks.

SECTION C - FACILITY SECURITY

8. Access control.

   a. Guards (military) (civilian).

   b. Assigned personnel.

      (1) Clearances.

      (2) Communications.

      (3) Emergency procedures.

      (4) Reserves.

9. Windows (number and type).

10. Ventilation ducts (number and type).

11. Construction.

    a. Walls.

    b. Ceiling.

    c. Floor.

12. False Ceiling.

    a. Type (fixed or removable).

    b. Distance between false and true ceilings.

13. Remarks.

SECTION D - DOORS

14. Number of entrances.

15. Type of doors used.

    a. Vault doors (manufacturer, model number, class).

    b. Wood (thickness/hollow/solid).

    c. Wood with metal (thickness of both door and metal covering; hollow, solid, metal on both sides).

    d. Metal (thickness/hollow/honeycomb).

    e. Frame.

    f. Other.

16. Number and types of doors used for emergency exits.

    a. Vault door (manufacturer, model number, class).

    b. Wood (thickness/hollow/solid).

    c. Wood with metal (thickness of both door and metal covering; hollow, solid, metal on both sides).

    d. Metal (thickness/hollow/honeycomb).

    e. Frame.

    f. Other.

17. Type of lock (entrance).

a. Combination (manufacturer, model number).

b. Is entrance door (if not a vault door) and/or the access control door equipped with a door closer? Yes _____ No _____ (If no, why not?)

18. Locks on windows and other openings.

19. Have hinges been properly secured on door opening outward? Yes _____ No _____ How?

20. Type of locking device used on emergency exits.

a. Lock (manufacturer, model number).

b. Metal strap or bar (size and thickness).

c. Security deadbolt(s).

d. Panic hardware.

e. Other (describe).

21. Number and types of doors used for emergency exits.

a. Electronic cypher lock (manufacturer, model number).

b. Mechanical cypher lock (manufacturer, model number).

c. Key lock (manufacturer, model number).

d. Electronic release (manufacturer, model number).

e. Guard.

f. Other.

22. Is combination lock of vault door or locally fabricated door opening into a nonsecure area protected against tampering?

No _____ Why not? Yes _____ Why not?

23. Combination changed by.

24. Combination on file at.

25. Double check system.

26. Remarks.

SECTION E - CONTAINERS

27. General Services Administration (GSA) approved, Class _____ Quantity of each _____.

28. Non-GSA approved, manufacturer, model, type of lock.

29. Open/closed signs.

30. Combination changed by.

31. Combination filed at.

32. Double check system.

33. Remarks.

SECTION F - ALARM PROTECTION

In all cases where applicable, give manufacturer and model numbers in answering the following questions.

34. Door protection.

    a. Balanced magnetic door switch.

    b. Closed circuit television.

    c. Heat detector.

    d. Lacing.

    e. Capacitance.

    f. Other.

35. Window protection.

    a. Alarm Tape.

    b. Switch.

    c. Capacitance.

    d. Closed-circuit television.

    e. Other.

36. Perimeter wall protection:

a. Vibration detection.

b. Lacing.

c. Capacitance.

d. Other.

37. Interior protection (within the facility, below false ceiling).

a. Volumetric alarm system.

b. Closed circuit television.

c. Other.

38. Ventilation and duct protection--

a. Barriers.

b. Breakwire alarms _____, duct trap.

c. Capacitance.

d. Other.

39. Overheard protection (space above false ceiling).

a. Volumetric alarm system.

b. Vibration detection.

c. Alarm lacing.

d. Other.

40. Perimeter (fence) protection.

a. Fence alarm.

b. Capacitance.

c. Closed-circuit television.

d. Tele-approach.

e. Seismic.

f. Guards and/or sentry dogs.

41. Transmission line supervision.

    a. Rigid or flexible conduit.

    b. Low security.

    c. High security.

    d. Other.

42. Guard response time for an alarm?

    When last tested?

43. Are all alarms operational?

44. Is emergency/backup power available for the alarm system?

45. Location of alarm annunciator panel?

46. Is the alarm system equipped with a "Remote Test" feature?

47. Are all alarm control units, sensors, and associated components equipped with tamper circuits? Yes_____ No_____ Why not?

48. Is tamper circuit operational?

49. Is procedure established for periodic testing of alarms?

50. When last tested?

    By whom?

51. Description of test methods.

52. Is the facility located in an area that is subject to burglarious attack and/or mob violence? (Describe kind of threat.)

53. Provide current assessment of hostile intelligence threat against facility. (Usually obtainable from local supporting military intelligence unit/representative.)

REQUEST FOR VISIT AUTHORIZATION

AMC SUP 1, AR 380-5

		DATE:
THRU:	**TO:**	**FROM:**

Permission is requested for the following named employee(s) tovisit your facility as described below:

LINE NO.	NAME OF VISITOR	DATE AND PLACE OF BIRTH	SSN	CITIZENSHIP

CLASSIFICATION OF INFORMATION TO BE DISCUSSED AND PURPOSE OF VISIT:

DATE(S) AND DURATION OF VISIT:

PERSON(S) TO BE VISITED:

TYPED NAME & TITLE OF REQUESTING OFFICIAL:	**SIGNATURE:**

TO BE COMPLETED BY SECURITY OFFICE

LINE NO.	LEVEL OF CLEARANCE AND ISSUING AUTHORITY	DATE

Unless otherwise notified, the above visit will be considered approved.

TYPED NAME & TITLE OF SECURITY OFFICER:	**SIGNATURE:**	**DATE:**

AMC FORM 1663-R-E
15 JAN 92

Previous editions of this form may not be used.

DATA REQUIRED BY THE PRIVACY ACT OF 1974
(5 USC 552a)

TITLE OF FORM	PRESCRIBING DIRECTIVE
Request for Visit Authorization	AMC SUP 1, AR 380-5

1. AUTHORITY
Executive Orders 10450 and 10865; Title 10, USC, Section 3012

2. PRINCIPAL PURPOSE
To advise facilities of forthcoming visits of military and civilian personnel.

3. ROUTINE USES
Indicates that a forthcoming visit is authorized and verifies the visitor's level of clearance and issuing authority. Provides facility being visited with the visitor's name; date and place of birth; Social Security Number; citizenship; classification of information to be discussed and purpose of visit; date(s) and duration of visit; and person(s) to be visited.

4. MANDATORY OR VOLUNTARY DISCLOSURE AND EFFECT ON INDIVIDUAL NOT PROVIDING INFORMATION
Disclosure of the information is voluntary. The personal information requested is necessary to preclude unauthorized disclosure of classified defense information. Refusal to provide information will result in nonadmittance to classified areas and briefings.